

1 Presented to the Court by the foreman of the
2 Grand Jury in open Court, in the presence of
3 the Grand Jury and FILED in The U.S.
4 DISTRICT COURT at Seattle, Washington.

5 *APR 16* 20⁰⁹
6 BRUCE RIFKIN, Clerk
7 By *[Signature]* Deputy

8 UNITED STATES DISTRICT COURT
9 WESTERN DISTRICT OF WASHINGTON
10 AT SEATTLE

11 UNITED STATES OF AMERICA,

12 Plaintiff,

13 v.

14 FREDERICK EUGENE WOOD,

15 Defendant.

CR09 0094 JLR
CASE NO.

INDICTMENT



09-CR-00094-INDI

17 The Grand Jury charges that:

19 **COUNT ONE**

20 **(Wire Fraud)**

21 **A. Background**

22 At all times material herein,

23 1. FREDERICK EUGENE WOOD was a resident of Seattle, in the Western
24 District of Washington.

25 2. The computer servers hosting the Craigslist website were located in San
26 Francisco, California, and Scottsdale, Arizona.

1 3. FREDERICK EUGENE WOOD devised and effected a wire fraud
2 scheme, described below, which included the use of Limewire, a "peer-to-peer"
3 computer "file sharing" program.

4 4. Peer-to-peer computer programs enable their users to create
5 decentralized, peer-to-peer ("P2P") networks of computers. P2P networks provide a
6 ready-made infrastructure for electronic file sharing by which files stored electronically
7 on any computer that is part of the network can be "published" or "shared" with any
8 other computer that is a member of the network, regardless of the physical location of
9 the respective computers.

10 5. P2P networks and file sharing programs can be used legitimately for
11 authorized and legal file sharing. P2P networks are, however, also known for, and
12 commonly used to facilitate the unauthorized and illegal replication of copyright-
13 protected music and videos files, among network members.

14 6. For individuals who are using a P2P network and program to share and
15 replicate music and video files, it is beneficial to run the program constantly, and to
16 configure any computer security protection firewalls to treat the P2P program as a
17 "trusted" program. This configuration negates the protection normally afforded by
18 firewall and anti-virus programs.

19 7. Limewire is a P2P file sharing program that can be downloaded, for free,
20 from a website on the Internet at www.limewire.com. The Limewire program's default
21 settings enable it to run constantly, and thereby to allow users constantly to share files.
22 The Limewire program also automatically configures firewall programs to view
23 Limewire as a trusted program, thereby negating the protection afforded by firewall
24 and anti-virus programs.

25 8. A number of P2P programs exist, and a number of different versions of
26 each program can exist. Some versions of some P2P programs have, by default, made
27 a user's entire computer hard drive accessible to other members of the P2P network.
28 Other versions of P2P programs, including the most recent version of Limewire, allow

1 a user to create a folder on the user's computer's hard drive entitled, "shared," in
2 which the user can place files he/she wishes to share. If the user is inexperienced or
3 not attentive, however, any file stored on the computer can be mistakenly included in
4 the "shared" folder. Computer "viruses" also exist which can effectively expand
5 access by a P2P network member to data beyond that stored in the designated "shared"
6 folder.

7 **A. The Offense**

8 9. Beginning at a date uncertain, but in or about July, 2007 and continuing
9 until on or about July 31, 2008, within the Western District of Washington and
10 elsewhere, FREDERICK EUGENE WOOD did knowingly and willfully devise and
11 intend to devise a scheme and artifice to defraud, and for obtaining money and property
12 by means of material false and fraudulent pretenses, representations, and promises; and
13 in executing and attempting to execute this scheme and artifice, did knowingly cause to
14 be transmitted in interstate commerce by means of wire communication certain signs,
15 signals, and sounds.

16 **B. Essence of the Scheme and Artifice to Defraud**

17 10. The essence of the scheme and artifice to defraud was that FREDERICK
18 EUGENE WOOD would use the P2P file sharing networks afforded by Limewire to
19 surreptitiously and illicitly steal identity (including social security number), and also
20 banking, financial and tax return information that had been stored by others on their
21 computers; that FREDERICK EUGENE WOOD would then use the identity and also
22 banking, financial and tax return information that belonged to others, without their
23 knowledge or consent, to produce counterfeit checks and also counterfeit driver's
24 licenses in the names of others, or to open, or attempt to open online credit accounts or
25 secure loans under the names of others; that FREDERICK EUGENE WOOD and
26 others would use the counterfeit checks in conjunction with the counterfeit driver's
27 licenses FREDERICK EUGENE WOOD had produced to fraudulently purchase
28 merchandise, including computers, or would incur charges on fraudulently opened

1 credit accounts; that FREDERICK EUGENE WOOD would use a computer and the
2 Internet to "post" advertisements for the sale of fraudulently purchased computers on
3 the "Craigslist" Internet website; that FREDERICK EUGENE WOOD would then sell
4 the fraudulently purchased computers to others, at a substantial discount, or, in some
5 cases, would purport to sell a computer that he had advertised for sale on Craigslist,
6 but would instead sell the would-be buyer a computer box containing something other
7 than a computer; and that once FREDERICK EUGENE WOOD had accepted funds for
8 the sale of these computers or computer boxes, he would convert the proceeds thereof
9 to his own personal use and benefit.

10 **C. The Scheme and Artifice to Defraud**

11 11. It was part of the scheme and artifice to defraud that FREDERICK
12 EUGENE WOOD knew that P2P programs, such as Limewire, are present on many
13 family and home computers, located across the nation and the world, and that the P2P
14 programs often are installed on those computers either by children, without the
15 knowledge or permission of their parents, or by adults who are themselves also
16 unaware that Limewire can make data and files stored on their computers accessible to
17 strangers who are part of the Limewire network.

18 12. It was further part of the scheme and artifice to defraud that FREDERICK
19 EUGENE WOOD knew that, with the use of his own computer and the Limewire P2P
20 network, he could under some circumstances access a wide range of information,
21 documents and data stored electronically on other computers hosting the Limewire
22 program, including social security numbers, bank statements and federal income tax
23 returns that had been stored electronically by other real people on and in their own
24 private computers. FREDERICK EUGENE WOOD knew that he could access
25 information on these computers regardless of their geographic location.

26 13. It was part of the scheme and artifice to defraud that FREDERICK
27 EUGENE WOOD utilized a computer in Seattle, Washington, containing P2P software
28 in order to facilitate and further his fraud scheme, with the result that his computer

1 would become part of an interstate P2P file sharing network that provided him with
2 direct peer-to-peer access, over the Internet, to other computers, on which the program
3 had been installed, regardless of their geographic location.

4 14. It was further part of the scheme and artifice to defraud that FREDERICK
5 EUGENE WOOD intended to, and successfully did, by means of interstate P2P
6 networks, surreptitiously gain access to identity and also banking, financial, and tax
7 return information of other, real people that had been stored electronically on their
8 private computers, without their knowledge, authorization, or consent, and that the
9 computers to which FREDERICK EUGENE WOOD thereby gained access were
10 located in many states, including Massachusetts, New York, Georgia, Florida, Ohio,
11 Iowa, Louisiana, Oregon and California.

12 15. It was further part of the scheme and artifice to defraud that FREDERICK
13 EUGENE WOOD did, through the use of the Limewire program, specifically "search"
14 within the computers of others for bank and financial statements, account information,
15 and federal income tax returns that had been stored electronically by other real people
16 on and in their own private computers.

17 16. It was further part of the scheme and artifice to defraud that FREDERICK
18 EUGENE WOOD would and did in turn use the identity, and also banking, financial,
19 and tax return information that he surreptitiously and illicitly obtained from the
20 electronically stored files on computers of other people to produce counterfeit checks
21 and driver's licenses containing identity and bank account numbers of other real people.
22 FREDERICK EUGENE WOOD used his computer to produce both the counterfeit
23 checks and the counterfeit driver's licenses.

24 17. It was further part of the scheme and artifice to defraud that FREDERICK
25 EUGENE WOOD would use the identity (including social security number
26 information), and also banking and financial information that he surreptitiously and
27 illicitly obtained from the electronically stored files on computers of other people to

1 open or attempt to open credit accounts "online," over the Internet, in the names of the
2 other real people whose identities he had stolen.

3 18. It was further part of the scheme and artifice to defraud that FREDERICK
4 EUGENE WOOD and others would use the counterfeit checks, together with the
5 counterfeit driver's licenses that FREDERICK EUGENE WOOD had produced, to
6 purchase merchandise, including computers.

7 19. It was further part of the scheme and artifice to defraud that FREDERICK
8 EUGENE WOOD would use a computer and the Internet to "post" advertisements for
9 the sale of fraudulently purchased computers on the "Craigslist" Internet website.

10 20. It was further part of the scheme and artifice to defraud that once
11 FREDERICK EUGENE WOOD had arranged, via Craigslist and then through
12 subsequent e-mail communications for a sale of fraudulently purchased merchandise, he
13 would instruct the would-be buyer to meet him at a location in the Seattle,
14 Washington, area.

15 21. It was further part of the scheme and artifice to defraud that, in some
16 instances in which he had arranged to sell a computer to a would-be buyer,
17 FREDERICK EUGENE WOOD would accept the agreed upon funds for the sale from
18 the would-be buyer, but in return for those funds, FREDERICK EUGENE WOOD
19 would give the would-be buyer a sealed computer box, that contained a book and/or
20 other objects, instead of a computer.

21 D. **Execution of the Scheme and Artifice to Defraud**

22 22. On or about November 14, 2007, within the Western District of
23 Washington and elsewhere, for the purpose of executing and attempting to execute this
24 scheme and artifice to defraud, FREDERICK EUGENE WOOD knowingly caused
25 to be transmitted in interstate commerce by means of wire communication, certain
26 signs, signals, and sounds, that is, an electronic posting over the Internet to the
27 Craigslist website of an advertisement for the sale of a MacBook Pro 15.4" Matte
28 computer, 2.2 GHz 2.0 GB RAM, for a price of \$1500.00, which computer

1 FREDERICK EUGENE WOOD thereafter agreed, via e-mail communications, to sell
2 to D.M., of Seattle, Washington, for \$1500.00, and for which sale FREDERICK
3 EUGENE WOOD took and received \$1500.00 from D.M. on November 15, 2007, but
4 in exchange for which funds FREDERICK EUGENE WOOD provided to D.M. a
5 computer box, containing only a book and a glass vase, instead of a computer.

6 All in violation of Title 18, United States Code, Section 1343.

7

8 **COUNT 2**

9 **(Accessing Protected Computer without Authorization to Further Fraud)**

10 1. Paragraphs 1 through 22 of Count 1 are realleged and incorporated as if
11 fully set forth herein.

12 2. On or about October 31, 2007, through on or about November 25, 2007,
13 within the Western District of Washington and elsewhere, FREDERICK EUGENE
14 WOOD knowingly and with intent to defraud, accessed protected computers without
15 authorization and in excess of authorization, and by means of such conduct furthered an
16 intended fraud by obtaining identity and banking information that belonged to R.M., of
17 Staten Island, NY, and identity and banking information that belonged to C.C., of
18 Warren, OH, which information FREDERICK EUGENE WOOD then used
19 fraudulently to counterfeit checks, and which counterfeit checks FREDERICK
20 EUGENE WOOD and others then used, in turn, fraudulently to purchase merchandise
21 exceeding \$5,000 in value within a period of one year.

22 All in violation of Title 18, United States Code, Section 1030(a)(4) and
23 (c)(3)(A).

24

25 **COUNT 3**

26 **(Aggravated Identity Theft)**

27 1. Paragraphs 1 through 22 of Count 1 are realleged and incorporated as if
28 fully set forth herein.

1 2. On or about October 31, 2007, within the Western District of Washington
2 and elsewhere, FREDERICK EUGENE WOOD knowingly transferred, possessed and
3 used, without lawful authority, a means of identification of another person, to wit, the
4 personally identifiable bank account number of R.M., of Staten Island, NY,
5 during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c),
6 to wit, Fraud and Related Activity in connection with Computers, in violation of Title 18,
7 United States Code, Section 1030(a)(4).

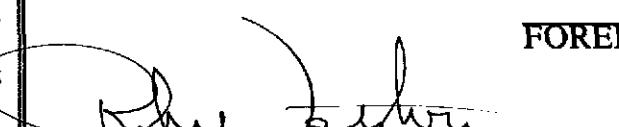
8 All in violation of Title 18, United States Code, Section 1028A(a)(1).

9
10 A TRUE BILL:

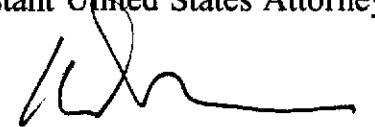
11 DATED:

12 Signature of the Foreperson redacted pursuant to
13 the policy of the Judicial Conference

14 FOREPERSON

15 
16 JEFFREY C. SULLIVAN
17 United States Attorney

18 
19 CARL BLACKSTONE
20 Assistant United States Attorney

21 
22 KATHRYN A. WARMA
23 Assistant United States Attorney